Feldgen, María

"Internet de las Cosas" y los ciudadanos

Tecnología & Sociedad, Nº 7, 2018
Revista del Centro de Estudios sobre Ingeniería y Sociedad
Facultad de Ingeniería y Ciencias Agrarias

"Internet de las Cosas" y los ciudadanos

María Feldgen[1]

RESUMEN

Internet de las Cosas (IoT) integra todo tipo de dispositivos inteligentes, inclusive ubicuos y autónomos, para crear soluciones más atractivas para las personas y los mercados. Promete la integración de múltiples ecosistemas empresariales existentes y emergentes para crear nuevos modelos de negocios con mayor rentabilidad y con más información de mejor calidad. La Unión Europea y Estados Unidos son los dos bloques económicos que están impulsando esta tecnología con concepciones completamente diferentes, pero con el mismo objetivo: IoT es para beneficio de la sociedad. En este trabajo se analizan los criterios y la valorización del derecho a la privacidad y la protección de datos personales de manera segura, asociado a la responsabilidad moral de quienes tienen acceso a los datos personales desde el punto de vista de las propuestas de estos bloques, sus sociedades, su impacto en sus propios ciudadanos y en países con una legislación fuerte de protección del ciudadano.

PALABRAS CLAVES

Internet de las Cosas, privacidad, protección de datos personales, seguridad, responsabilidad moral.

[1] Computadora Científica (Universidad de Buenos Aires), International Engineering Educator (International Society for Engineering Education), Profesora Asociada e Investigadora jubilada (Facultad de Ingeniería, Universidad de Buenos Aires), Profesora Titular jubilada (Facultad de Ingeniería y Ciencias Agrarias, Universidad Católica Argentina), miembro de la IEEE Argentina. maria.feldgen@gmail.com

ABSTRACT

The Internet of Things integrates all kinds of intelligent devices, including ubiquitous and autonomous, to create more attractive solutions for people and markets. It promises the integration of multiple existing and emerging business ecosystems to create new business models with greater profitability and with more information of better quality. The European Union and the United States are the two economic blocs that are driving this technology with completely different conceptions, but with the same objective: IoT is for the benefit of society. This paper analyzes the criteria and the valuation of the right to privacy and the protection of personal data in a secure manner, associated with the moral responsibility of those who have access to personal data from the point of view of the proposals of these blocks, their societies, their impact on their own citizens and in countries with strong citizen protection legislation.

KEYWORDS

Internet of Things, privacy, protection of personal data, security, moral responsibility.

1. INTRODUCCIÓN

La International Organization for Standarization, en el artículo "How the Internet of Things will change our lives" de Elizabeth Gasiorowski-Denis (2016), comienza diciendo: "La Internet de las Cosas tiene el poder de cambiar nuestro mundo. Y mientras comenzamos a ver su increíble impacto, recién estamos al inicio de este viaje de transformación". En el artículo se cita al tecnólogo Chuck Evanhoe:

> IoT será un gran facilitador para tener mejor información tanto para el consumidor como para el ambiente comercial. Creo que el impacto de IoT será general. Todos los sistemas en los que no pensamos en nuestra vida cotidiana serán más efectivos para mantener productivos a los seres humanos, por lo que el impacto no será solo en un área. […] Desde "electrodomésticos inteligentes" hasta "fábricas inteligentes", tendremos mejor información, más control y conocimiento de las cosas cotidianas que necesitamos para funcionar, tanto conocidas como desconocidas.

De la empresa Intel (2016) dirigido a las empresas:

> Cada producto, cada proceso, cada persona y cada lugar deja un rastro de datos, y ese rastro de datos puede ser capturado, rastreado, compartido, combinado, extraído y analizado. El resultado genera nuevas formas de mejorar y comprender, no solo sus propias operaciones, sino también lo que los consumidores quieren, lo que necesitan, cómo ofrecérselos, y cuánto están dispuestos a pagar por ello. Datos agregados de múltiples fuentes más dispositivos pueden convertirse en ideas únicas que pueden inspirar nuevos productos y servicios, que mejoren las vidas de los consumidores y la forma en que experimentan el mundo, ya sean parte del envejecimiento demográfico de Occidente, o la floreciente clase media en una economía emergente.

Otros artículos semejantes y sesiones temáticas, como la de la HiPEAC Europea (2015) titulada "Internet of Things: technology and applications for a good society" predicen cómo las sociedades y sus ciudadanos se van a beneficiar de esta tecnología. Esta innovación disruptiva se puede describir desde dos puntos de vista.

Desde el punto de vista de la tecnología, IoT es disruptiva porque integra todo tipo de dispositivos inteligentes, inclusive ubicuos y autónomos, para crear soluciones más atractivas para las personas y los mercados. Promete la integración de múltiples ecosistemas empresariales existentes y emergentes para crear nuevos modelos de negocios con mayor rentabilidad y con mejor calidad y cantidad de información para formar un gran ecosistema de alcance global. Cada integrante de este ecosistema complejo será, a su vez un sistema complejo al igual que su sistema o capa de interconexión. Una estructura tan compleja presenta múltiples riesgos de todo tipo, tanto conocidos como inciertos. Dentro de estos riesgos se destacan aquellos bien conocidos de la Internet actual y otros nuevos que atentan contra la privacidad de las personas y contra el objetivo de IoT de beneficiar a los ciudadanos. Por lo tanto, para prevenir estos riesgos se deben tener en cuenta las cuestiones legales relacionadas con la protección de datos y la ley de privacidad (Nicolescu *et al.*, 2018; Fabiano *et al.*, 2017).

Desde el punto de la vista de la filosofía, IoT es disruptiva porque es un conjunto de nuevas tecnologías generalizadas y omnipresentes en el mundo digital que difiere de las tecnologías de la información tradicionales (Yoo *et al.*, 2010). Además, esta evolución de la tecnología requiere de la inclusión de nuevas teorías y disciplinas en un marco

extendido de SCOT, denominado SCODT, que Van Baalen *et al*. (2018) describen como:

> Es una nueva realidad. […] Es una nueva etapa de evolución de las TI que obliga a reconsiderar y reconceptualizar estrategias tradicionales y de pensamiento. Este papel emergente de las TI ha sido acompañado con un interés creciente en la adopción de ecosistemas como lente analítica, lo que lleva a la inclusión de teorías y conceptos de otras disciplinas como la complejidad, la biología, la teoría de la innovación y la economía. Estas "nuevas" teorías en la investigación de TI pueden ser útiles para explicar la complejidad, la conexión y dinámica de las tecnologías digitales. Sin embargo, tienden a permanecer en silencio sobre las opciones humanas en el contexto del desarrollo y construcción de estas nuevas tecnologías. Es decir, la agencia permanece "sin teorizar" cuando se investiga la naturaleza, la construcción y las consecuencias de las tecnologías. […] SCOT podría respaldar la investigación en este sentido, pero el estudio de la construcción social de la tecnología en el mundo digital requiere que se amplíe este marco para tener en cuenta la naturaleza de las tecnologías que sustentan los ecosistemas digitales, las individualidades interconectadas como partes interesadas activas, el contexto socio-digital y la interacción entre las personas y las tecnologías digitales (SCODT).

Sin duda, es disruptiva en todos los sentidos porque requiere nuevos enfoques tanto desde la perspectiva tecnológica como desde la perspectiva de la filosofía en un contexto sociodigital de alcance global. Los dos bloques económicos que promueven y están iniciando el desarrollo de esta tecnología son la Unión Europea (UE) y Estados Unidos (EE. UU.). La propuesta de la UE y sus planes de desarrollo tienen una perspectiva filosófica/sociológica/tecnológica del desarrollo de la IoT, en la cual el ciudadano tiene un papel preponderante. La propuesta de Estados Unidos, por el contrario, se presenta como un desarrollo tecnológico tradicional, en la cual los negocios tienen un papel predominante.

Son dos propuestas con concepciones muy diferentes, sin embargo, toda la publicidad asociada a ellas, sus definiciones y promesas ponen énfasis en que es "para el beneficio de la sociedad" y "que se prioriza la privacidad y la seguridad". Ambos bloques económicos son occidentales, pero sus sociedades son muy diferentes, como también los criterios y valorización del derecho a la privacidad y a la protección de sus datos personales de manera segura, y la responsabilidad moral de quienes tienen acceso a los estos. En este trabajo se analizan ambas propuestas.

2. CARACTERÍSTICAS DE LAS SOCIEDADES DE AMBOS BLOQUES

Hay características muy diferentes en ambos bloques que influyen en cómo el gobierno, las empresas, los expertos y la sociedad promueven y proponen construir este ecosistema, y la importancia que tiene la privacidad y protección de los datos, la seguridad de la información y la responsabilidad moral asociada.

Una razón surge de una divergencia básica de actitud de las personas, su confianza en la tecnología y en sus desarrolladores. Los europeos tienen una profunda desconfianza en las corporaciones e individualmente esperan que el Estado cuide a todos. Mientras que a los estadounidenses les preocupa más que su gobierno invada su privacidad. Individualmente, es más importante tener libertad para lograr sus objetivos y ejercer el derecho a elegir que el Estado asegure las necesidades básicas de todos los ciudadanos (Sullivan, 2006).

Además, hay un abismo en la forma en que las empresas tecnológicas estadounidenses ven la regulación de cualquier tipo. Consideran que la regulación es fundamentalmente incompatible con la innovación. En Europa, por otra parte, la regulación se considera fundamental para proteger la equidad y la competencia. Lo mismo se aplica para los negocios y los mercados (O'Brien, 2018).

La UE, a través de la Comisión Europea, fija políticas y marcos reguladores para la investigación, el control del desarrollo y la inserción de nuevas tecnologías correspondientes a las TIC para todos sus países miembros. Esta postura es compartida por China, Japón y Corea del Sur. Para la IoT tiene un plan estratégico específico de investigación para fijar las recomendaciones que sean necesarias para guiar a Europa a su manera y de tal forma que sea en beneficio para todos sus ciudadanos. IoT es una tecnología de la información y la comunicación (TIC) y por consiguiente, es un producto cultural que requiere del análisis de su impacto social y ambiental. Es fundamental preservar la privacidad y protección de los datos personales porque en la legislación europea "es un derecho humano", tal como lo es la protección del medio ambiente, la salud humana, la sustentabilidad y la conveniencia social. El paradigma europeo es que la investigación y el desarrollo deben ser un emprendimiento compartido entre políticos, expertos, empresas y fundamentalmente la sociedad de toda la UE.

En cambio, en Estados Unidos, el paradigma es que sean emprendimientos independientes de las grandes corporaciones y empresas agrupadas en alianzas y consorcios que fijan sus propias propuestas de IoT. Hay participación, no vinculante, de organizaciones de estándares y del gobierno para promover el desarrollo de esta tecnología. Por ejemplo, la función del NIST (CPS-PWG, 2017) y del Sens (Infosec Institute, 2017) es crear grupos de expertos para asesorar a las empresas y al gobierno en su uso de IoT. En este contexto Sens presentó una ley para el desarrollo de la innovación y crecimiento de IoT: DIGIT Act, (2017). La ITU (Unión Internacional de Telecomunicaciones) está definiendo estándares para los protocolos de redes y dispositivos (ITU-T Y.2060, 2012; ITU IoT, 2005). La participación gubernamental de la administración actual corresponde a la FTC (Comisión Federal de Comercio), que es la responsable de "proteger a los consumidores y promover la competencia" desde el punto de vista de la protección de la privacidad en línea. La FTC (FTC Report, 2015) manifiesta que aún no es necesaria su participación activa, aunque admite que es probable que sean mayores los riesgos contra la seguridad y privacidad. Pero al evaluar el equilibrio correcto entre proteger a los consumidores y optimizar la innovación como el mayor desafío de IoT, considera que es conveniente apoyar a las empresas que tienen una autorregulación voluntaria fuerte y de mejores prácticas en lugar de imponer estándares estrictos. En todos los casos, las referencias son a "consumidores" (en lugar de ciudadanos) y desde el punto de vista del "ambiente comercial o de los negocios".

Con respecto a la responsabilidad moral que tienen las organizaciones con respecto a la privacidad, protección de datos de ciudadanos, seguridad de esos datos y los riesgos, la UE tiene leyes y reglamentaciones obligatorias, por ejemplo, la EU GDPR (2018) (Reglamento General de Protección de Datos), que entró en vigencia el 25 de mayo de 2018 (y que reemplaza a la Directiva de Protección de Datos 1995/46/CE), que deben cumplir todos los productos que se desarrollen y se pretendan comercializar en la UE. Se basa en el principio de que los datos personales son propiedad del ciudadano. En cambio, en Estados Unidos no existe una protección legal para datos personales que regule la recopilación y el procesamiento de estos datos. La protección de datos está parcialmente regulada por muchas leyes estatales y federales y por las promesas de las alianzas comerciales para mantener la confianza de los consumidores.

Estas diferencias probablemente provengan de su historia. En la UE, donde las personas han tenido dictaduras, la protección de datos (y la privacidad) se declara como un derecho humano y está regulado por una legislación integral. Por el contrario, en Estados Unidos, la actitud hacia la protección

de datos se rige principalmente por el mercado. Además, con la adopción de la Ley Patriótica en respuesta a los sucesos del 11 de septiembre de 2001, se redujeron significativamente las restricciones en la recopilación de datos personales por parte de los organismos encargados de hacer cumplir la ley (Roessler *et al*., 2013; Dimov, 2013; Sullivan, 2006).

De la misma forma, los conceptos de evaluación de riesgos se manejan de manera diferente en los dos lados del Atlántico (Jasanoff, 2000). El lenguaje de la regulación de riesgos de Estados Unidos está "basado en la ciencia" y el análisis de costo-beneficio tiende a ser cuantitativo, impulsado por un razonamiento económico y puede ser abiertamente tecnocrático en sus implicaciones políticas. Los europeos dan un lugar a la historia, la sociología y la filosofía analizando los riesgos desde dos puntos de vista: los riesgos bien definidos o conocidos se analizan según el Principio de Prevención, aplicando técnicas de análisis de costo-beneficio priorizando los aspectos sociales sobre los económicos (Whiteside, 2006), con cursos de acciones cuidadosamente planificadas. Para el manejo de riesgos inciertos, el proyecto PRESCIENT del EU RRI (2012) recomienda que la precaución es el mejor marco teórico de acción ante los riesgos inciertos y que es necesario integrar el Principio de Precaución (PP) para evaluar el impacto de los riesgos inciertos contra la privacidad (Wright *et al*., 2011). En cambio, en Estados Unidos, se observa un fuerte rechazo a las regulaciones y a la previsión de riesgos, en especial al PP. La FTC resume comentarios con respecto a cuestiones de la privacidad del consumidor y la seguridad que impone la creciente conectividad, por ejemplo:

> Establecer escenarios de los peores casos sobre el mal uso de algunas tecnologías IoT puede inducir a activistas políticos y legisladores a tratar de cambiar el curso o controlar su desarrollo. […] Las restricciones preventivas al desarrollo de IoT podrían retrasar la innovación tecnológica y limitar los beneficios que reciben los consumidores. En cambio, los formuladores de políticas deberían ejercer moderación y humildad frente a los cambios inciertos y abordar los daños que se desarrollan, si es que ocurren, después de un análisis cuidadoso de los beneficios y costos de varios remedios (Thierer, 2013).

Mucho más que los legisladores estadounidenses, los europeos abordan los asuntos medioambientales y también tecnológicos usando un lenguaje de "deber", "cuidado" y "participación democrática". No hay un lenguaje común para debatir sobre la protección y las acciones preventivas, tanto en medio ambiente como en tecnología, aun cuando se enfocan en problemas con posibles consecuencias globales (Whiteside, 2006).

3. IoT COMO UNA NUEVA TECNOLOGÍA EN BENEFICIO DE LA SOCIEDAD

Desde que la computación se aplica a los negocios, las personas son el foco principal y sus datos es el activo más valioso de una empresa (Hawley, 1995). IoT como ecosistema TIC integrará servicios comerciales y servicios esenciales que se requieren para vivir en la sociedad, tales como energía, agua, transporte, asistencia sanitaria, municipios y gobiernos, etc. Su gran capacidad de captura de información y de procesamiento, con nuevos sistemas de aprendizaje automático y analítico de datos tendrán mayor capacidad de influir en la toma de decisiones que pueden afectar a los individuos de la sociedad para bien o para mal. El ciudadano será aún más vulnerable que antes, si no se protegen sus datos adecuadamente. Además, de los desarrollos tecnológicos previos, se puede decir que la privacidad y la ética no fueron aspectos naturales a considerar en la agenda de la tecnología (Almeida *et al.*, 2015).

Los cambios tecnológicos y su impacto en la sociedad dieron un fuerte impulso, en las últimas dos décadas, a la Filosofía de la Información o de la Tecnología de la Información desde el punto de vista ético de los ciudadanos más que de los consumidores. Floridi, en la introducción de su libro *The Philosophy of Information* (2011), resume la evolución de estos cambios tecnológicos:

> Más de medio siglo después de la construcción de los primeros *mainframes*, la sociedad ha llegado a un punto en el que los problemas relacionados con la creación, la dinámica, la gestión y la utilización de la información y los recursos computacionales son vitales. […] Ninguna generación anterior ha estado alguna vez expuesta a una aceleración tan extraordinaria del poder tecnológico sobre la realidad con los correspondientes cambios sociales y responsabilidades éticas. […] Las sociedades postindustriales más desarrolladas literalmente viven de la información, y las TIC es lo que las mantiene constantemente oxigenadas.

Cada vez que se anuncia una nueva TIC, los filósofos y los tecnólogos/científicos se hacen la pregunta: ¿cuál será el impacto de todas estas nuevas TIC sobre la condición humana y el medio ambiente? Para responderla, la Agenda Digital de la Unión Europea (EU Digital Agenda, 2014), y desde el punto de vista del pensamiento filosófico, organizó el proyecto de investigación llamado "The onlife initiative: concept reengineering for rethinking societal concerns in the digital transition". Fue el comienzo en la UE de un proceso de reflexión sobre qué significa una era hiperco-

nectada integrando a toda la UE, sus gobiernos, universidades, empresas y principalmente ciudadanos. El resultado del proyecto fue el libro *The onlife manifesto* (Floridi, 2015) que recopila las conclusiones filosóficas de 15 académicos en antropología, ciencia cognitiva, informática, ingeniería, derecho, neurociencia, filosofía, ciencia política, psicología y sociología. Fue un ejercicio de pensamiento colectivo para explorar las consecuencias relevantes de esos cambios para la política.

Una de las contribuciones muy importantes del *Manifiesto* es que brinda una visión de cómo

> El despliegue de las TIC y su adopción por parte de la sociedad afectan radicalmente la condición humana, en la medida en que modifican nuestras relaciones con nosotros mismos, con los demás y con el mundo. La omnipresencia constante de las TIC sacude los marcos de referencia establecidos a través de las siguientes transformaciones:
>
> i. la difuminación de la distinción entre realidad y virtualidad;
> ii la difuminación de las distinciones entre humano, máquina y naturaleza;
> iii la reversión de la escasez de información a la abundancia de información; y
> iv el cambio de la primacía de las entidades a la primacía de las interacciones (Floridi, 2015).

Dos de los pensamientos del *Manifiesto* reflejan algunas de las preocupaciones sobre cómo esta tecnología afectará a la sociedad. En el capítulo 1, "¿Fin de la modernidad?: ideas que obstaculizan la capacidad de la formulación de políticas para enfrentar los desafíos de una era hiperconectada", se refiere a cómo las TIC desafían los supuestos de la ética llamando a nociones de responsabilidad distribuida.

La utilización de la información por parte de las TIC ha sido durante mucho tiempo objeto de debate público y académico con respecto a la privacidad y protección de datos personales, en conjunto con la seguridad de la información y las amenazas a estos últimos. La privacidad es un valor social, es algo que todas las personas valoran, es importante para un sistema político democrático y no se puede tener a menos que trabaje toda la sociedad en conjunto (Reagan, 1995). Spiros Simitis (1987) describió la privacidad como un elemento constitutivo de una sociedad democrática; y Ruth Gavison (1980) lo refuerza al indicar que la privacidad también es esencial para el gobierno democrático porque fomenta e

incrementa la autonomía moral del ciudadano, que es un requisito central de una democracia (Roessler *et al*., 2013).

En el capítulo 2, "En la esquina de Frankenstein y Gran Hermano: miedos y riesgos en una era hiperconectada", dice:

> Los miedos y los riesgos también pueden percibirse en términos de control: demasiado control, a expensas de la libertad, o a la falta de ella, a expensas de la seguridad y la sostenibilidad. […] Responsabilidades distribuidas e intrincadas pueden entenderse erróneamente como una licencia para actuar de manera irresponsable; estas condiciones pueden tentar aún más a los líderes empresariales y gubernamentales a posponer decisiones difíciles y, por lo tanto, a que se pierda la confianza.

La responsabilidad moral implica que los principios de prevención y precaución son ineludibles. Los requerimientos de privacidad y protección de datos personales de personas físicas y jurídicas, y la seguridad de la información se deben considerar desde la concepción y durante todo el ciclo de vida de la tecnología. Al igual que la protección del medio ambiente y salud humana, sustentabilidad y conveniencia social. Es una tecnología nueva y estamos en un estado inevitablemente experimental, y esto generalmente no está a la vista del público ni de la negociación pública. Además, no se debe usar a los ciudadanos como sujetos experimentales sin su consentimiento en experimentos desconocidos porque se están creando problemas éticos y sociales serios (Felt *et al*., 2007). Almeida *et al*. (2015) destacan que estas características son esenciales para generar la confianza necesaria en este ecosistema, haciéndolo compatible con los derechos humanos y asegurando que se desarrolle a la medida, y no a expensas, de las personas.

4. LA ÉTICA EN LAS PROPUESTAS DE LA UE Y LOS EE. UU.

4.1 Quién decide qué se va a producir, cómo y para quién

En la UE es más importante el tema social que los problemas metodológicos y de la construcción de IoT. La Comisión Europea lidera el desarrollo a través de sus programas Horizon 2020, las Políticas para Investigación e Innovación (European Commission, 2012) y la recomendación de la Investigación e Innovación Responsable (EU RRI, 2012) para TIC. El *Cluster of European Research Projects on IoT* (CERP-

IoT, 2009) es el plan estratégico específico de investigación para el futuro ecosistema basado en la RRI. En ellos se definen los marcos éticos con un fuerte énfasis en la privacidad, protección de datos personales y seguridad de la información, entre otros valores importantes para una sociedad, y los procedimientos. En todos los procedimientos y recomendaciones, los pensamientos del *Manifiesto* están presentes para inducir a la reflexión sistemática de las consecuencias de esta tecnología para la vida humana. Hay fuertes lazos con los filósofos y sociólogos de la Escuela de Frankfurt (Herbert Marcuse, Theodor W. Adorno y Max Horkheimer), Jürgen Habermas, Jacques Ellul y Langdon Winner (Reydon, 2017). Por ejemplo, en la RRI se le da mucha importancia a la pregunta central de este encuadre filosófico: si la tecnología nos controla o si somos capaces de controlar la tecnología (Feenberg, 2003; Dusek, 2006; Nye, 2006) que se refleja en los procedimientos y acciones necesarias para tratar con riesgos e incertidumbres y asegurar que se controla esta tecnología.

En cambio, en Estados Unidos, el enfoque es desde el punto de vista de la tecnología y los negocios usando la forma tradicional de desarrollar *software* y *hardware*, con múltiples propuestas de solución que ofrecen las alianzas y consorcios, que están condicionadas por quienes componen estas asociaciones de empresas. Corporaciones tecnológicas como Apple y Google trabajan independientemente, Intel y Cisco Systems se han unido. Otros han formado alianzas y consorcios en torno a diversos componentes de IoT, o sectores del mercado, en el cual compiten y simultáneamente comparten productos y servicios. Además, es notable la disposición que muestran empresas desconocidas de reconocer la supremacía de las grandes corporaciones buscando aliarse a estos o entre ellas para definir sus propias soluciones sin adherir a los estándares. Los analistas y consultores de tecnología condenan esta falta de consenso en el uso de protocolos e interfaces estándares porque aumenta la complejidad del sistema y los riesgos al comprometer la seguridad de todo el sistema y especialmente de los datos personales. Por ejemplo, las siguientes publicaciones muestran los resultados de los primeros experimentos y sus problemas. En el artículo "Gartner identifies the top 10 Internet of Things technologies for 2017 and 2018" (Gartner, 2017) se expresa:

> IoT exige una amplia gama de nuevas tecnologías y habilidades que muchas organizaciones aún no han dominado. Un tema recurrente en el ambiente de IoT es la inmadurez de las tecnologías y servicios, y de los proveedores que los proporcionan. […] En muchas de las áreas de tecnología, la falta de las habilidades necesarias también plantearán desafíos importantes.

El informe del IoTWF (2017) realizado por Cisco, que entrevistó a 1.845 responsables de toma de decisiones de TIC en Estados Unidos, Inglaterra e India, encontró que

> El 75 % de los proyectos de IoT fracasaron por falta de las habilidades necesarias y por implementaciones pobres dejando a las empresas desamparadas.

En la UE participan todos los interesados: expertos, políticos, empresa y la sociedad. El plan tiene una base filosófica multidisciplinaria, es progresivo y tiene una primera fase hasta el 2020 para que universidades y empresas trabajen en conjunto para entender cada problema y cuáles soluciones serían aceptadas por sus grupos sociales. Los fondos de investigación son controlados por todos los interesados. El contexto de la investigación coincide con el abordaje del ambiente SCODT en este nuevo mundo digital (Van Baalen *et al.*, 2018). En otras palabras, es una construcción social, con artefactos que son ecosistemas en un mundo digital. Esta construcción incluye la ética desde el comienzo, coincidiendo con Pinch *et al.* (2013), y en la cual los actores sociales y los innovadores se hacen mutuamente responsables con una visión sobre la aceptación, la sustentabilidad y la conveniencia social del proceso de innovación y sus productos comercializables (EU RRI, 2012). Durante todo el proceso hay una participación activa de los ciudadanos aplicando el concepto de gerenciamiento responsable y debates públicos tripartitos: sociedad, políticos y fabricantes, los que denominan la moderación al "jalar en la política" y "empujar en la tecnología" (con tal de evitar violaciones de ambas partes).

En Estados Unidos, no hay referencia a la participación activa de la sociedad. Hay discusiones en el ámbito político y de los grandes consultores de tecnología, corporaciones y alianzas. El objetivo es impulsar el desarrollo tecnológico para ganar el mercado de las "cosas". Si hay efectos dañinos o desastrosos se verá después cómo solucionarlos, lo cual puede ser muy costoso para remediarlos, como explica el dilema de Collingridge (Liebert *et al.*, 2010) e incluso que la sociedad rechace totalmente el producto. En Estados Unidos las fuerzas que moldean a las "cosas" son económicas, acompañadas por políticas de apoyo incondicional a las empresas.

Mientras que en la UE el tema central es la privacidad desde el punto de vista de la ética, en Estados Unidos lo es la confianza en el ecosistema y la privacidad se interpreta permanente en el contexto de la inseguridad.

Por ejemplo, la OTA en su artículo "Internet of Things. A visión for the future" (2017a) resalta:

> El aspecto más importante es la confianza del consumidor para que IoT prospere y crezca. […] Los miedos de los consumidores sobre la seguridad y la privacidad son citados como las dos barreras más importantes que enfrenta IoT dado que investigadores y actores maliciosos mostraron cómo un dispositivo puede ser inseguro y provocar un perjuicio colectivo.

Proponen como solución el despacho de dispositivos con "seguridad por defecto". Otro artículo de la OTA, "IoT security and privacy trust framework v2.5" (2017b), se refiere a la seguridad intrínseca de los dispositivos, desde el punto de vista de su construcción, venta y distribución. Por ejemplo, en el punto 32 dice que se debe

> Proveer la posibilidad de que el usuario pueda eliminar o hacer anónimos datos personales sensibles almacenados en los servidores de la empresa cuando se discontinúa el uso, se pierde o se vende el dispositivo.

El derecho que tiene una persona de solicitar que se eliminen datos de su persona es, en cualquier contexto, no solamente cuando no se usa más ese dispositivo. No es el mismo significado. Esta misma interpretación se observa también en el documento "IoT security and privacy risk considerations" de NIST (2017). No hay referencia al concepto de protección de los datos personales, ni a la responsabilidad formal dentro del contexto de la sociedad, sino que la interpretación es siempre desde el punto de vista del fabricante y del ambiente comercial.

4.2 Regulaciones e innovación. Experimentación inicial

El EU GDPR (2018) es el nuevo Código de Privacidad obligatorio acordado por todos los Estados miembros de la UE La premisa básica de este código es que los datos pertenecen a los usuarios. Por ejemplo, obliga a las empresas a revelar el alcance completo de la información que recopilan, cómo la usarán (derecho a explicación) y cómo la protegerán para evitar el acceso no autorizado. Ofrece a los usuarios la posibilidad de exigirle a una empresa que borre todos sus datos de sus servidores. Obliga a la "pseudominimización" de los datos (datos totalmente anónimos), esto implica que no debe existir forma alguna de relacionarlos con el usuario una vez ingresados al sistema. Fija la norma-

tiva para la prevención de todos los riesgos conocidos y define el alcance del concepto de privacidad de una persona.

El proyecto ETICA (EU ETICA, 2011), que justificó la inclusión obligatoria de la "Privacidad por diseño", también demostró que no es una restricción a la innovación tecnológica, sino que permite que estos avances sean realmente aceptados por la sociedad. Los ejemplos que menciona como justificación son el uso de la tecnología de imágenes corporales en los aeropuertos de Alemania: se cuestionó si la introducción era proporcional a los objetivos perseguidos con base en la Constitución; en Holanda, la instalación obligatoria de medidores inteligentes en los hogares para permitir la detección y optimización del uso de energía fue rechazada por violación de la privacidad al permitir que terceros pudieran monitorear los hogares. Estos cuestionamientos y las pérdidas económicas asociadas podrían haberse evitado si los actores de la sociedad hubiesen participado en el diseño inicial de esas tecnologías y en su experimentación.

La UE también proporciona los ambientes de experimentación con consentimiento y para los diferentes grupos sociales involucrados. Se basa en la Teoría ANT (Actor Network Theory, Latour, 2005), el encuadre es el de experimento social ético derivado de los principios bioéticos de no maleficencia, beneficio, respeto por las personas y justicia que propone Ibo van de Poel (2016). El fundamento es que una nueva tecnología es como un experimento del mundo real enfocado principalmente en la imposibilidad de predicción de riesgos, que requiere del principio del consentimiento informado, es decir, la aceptación de experimentos por parte de las personas (Kron *et al.*, 1994). Aunque, posiblemente, estos sean experimentos a pequeña escala, serían el primer paso para verificar que no se viola la ética, para analizar el impacto de nuevos riesgos y la forma de mitigarlos, aplicando y mejorando el Principio Precautorio. Una ventaja importante de compartir los ambientes de experimentación es que se puede aprovechar efectivamente la experiencia de las pruebas previas.

En Estados Unidos, la recopilación y el uso de datos personales no está regulado a nivel nacional. Es un sistema fragmentado de leyes y reglamentaciones federales y estatales que a veces se superponen, coinciden o se contradicen entre sí. Las leyes existentes se aplican a categorías especiales de datos, tales como información financiera, de salud, de menores de edad y de comunicaciones electrónicas. En 2017, en un reportaje de Sam Thielman (2017), la presidenta del FTC enfatizó que no es un ente regulador ni un organismo encargado de la aplicación de la ley. El enfoque actual es "esperar-y-ver". Con referencia a los datos personales:

la FTC defiende, por ejemplo, que *Big Data* pueda ofrecerle a los consumidores diferentes precios para el mismo producto. Por ejemplo, se permite que las aerolíneas y los hoteles alteren precios de servicios basándose en los datos del consumidor para fomentar la competencia. El principio que aplican es que la información se puede usar para ofrecer a algunos consumidores un precio más alto o para ofrecer a otros una mejor oferta. Además, se espera que los fabricantes de dispositivos de electrodomésticos decidan las mejores prácticas entre ellos, es decir, por autorregulación. La FTC coincide con la posición, denominada "un nuevo mundo con un sistema de legislación suave" (Thierer, 2017).

La política de Estados Unidos para IoT es lo que Adam Thierer (2017) denomina "Innovación sin restricciones" (*permissionless*), que se refiere a la noción de que la experimentación con nuevas tecnologías y modelos de negocios generalmente debería permitirse por defecto. A menos que se pueda argumentar convincentemente que traerá un perjuicio grave a la sociedad, se debe permitir que la innovación continúe sin interrupción y que los problemas, si es que se desarrollan, pueden abordarse más adelante. Con las redes sociales en Internet se procedió de esta forma, fueron experimentos sociales sin consentimiento de sus usuarios y algunas de sus violaciones de la ética fueron tema de la justicia o significaron el fracaso o un cuestionamiento serio de esa tecnología informática. Por ejemplo, en 2017 hubo un robo de datos personales en Equifax que afectó a 143 millones de personas; Yahoo! admitió que miles de millones de sus cuentas de correo electrónico se vieron comprometidas; la filtración accidental de datos personales de Deep Root Analytics de casi 200 millones de votantes estadounidenses y el intento de Uber de ocultar un robo de información que afectó a 57 millones de cuentas (O'Connor, 2018).

5. CONCLUSIONES

Una de las diferencias más marcada es la innovación sin restricciones estadounidense, cuyo objetivo es establecer las políticas públicas por defecto más permisivas, afirmando: 1) la innovación tecnológica es el determinante más importante del bienestar humano a largo plazo; 2) el aprendizaje a través de la experimentación continua por prueba y error es un valor real por la capacidad de recuperación y por la adaptación continua al cambio tecnológico; 3) limitar una nueva innovación debería ser el último recurso, no el primero. La innovación debería ser inocente hasta que se demuestre su culpabilidad; 4) con respecto a las

intervenciones regulatorias, la política debe basarse en la evidencia de un perjuicio potencial concreto y no en el peor de los casos hipotéticos y 5) si las políticas de intervención son realmente necesarias, las soluciones flexibles y de naturaleza *ex post* (de reacción) casi siempre son preferibles a los controles rígidos, de naturaleza *ex ante* (anticipatoria). Coincide con la política de la FTC de "un nuevo mundo gobernado por una legislación suave" (Thierer, 2017).

La posición política opuesta es la de la UE, con su enfoque muy centrado en la sociedad y los derechos de las personas, su historia y filosofía permiten que los temas del medio ambiente e IoT evolucionen en el mismo sentido, demostrando que la ética y el PP no deben verse como una restricción de los avances tecnológicos y hoy es el bloque más avanzado en el tema de ciudades /hogares/urbanismo inteligente de IoT (*smart cities*).

IoT pertenece a un mercado internacional, cada componente del ecosistema tiene que cumplir con las regulaciones que impone el país del ciudadano y ambiente del cual obtiene, procesa y almacena datos personales. Una de las virtudes más publicitadas de IoT es la adaptabilidad de sus componentes. Esta virtud ahora se está poniendo a prueba por las regulaciones de Protección de los Datos de la UE y de China [GDPR y las nuevas Especificaciones de los Estándares Nacionales en Seguridad Tecnológica y Seguridad de la Información Personal (Liao, 2018)] que entraron en vigencia en mayo de 2018. En ambos mercados, todo producto o servicio de Internet/IoT ofrecido a sus ciudadanos debe cumplir con las correspondientes regulaciones. La ética pasó a ser un requisito obligatorio con sanciones y punitorios muy onerosos por incumplimiento. Ambas regulaciones son similares pero con diferencias: la de China es más restrictiva que el GDPR con respecto al traslado de datos personales entre países y con respecto a cuáles considera datos personales.

La privacidad desde el diseño y por defecto es considerada una de las "mejores prácticas", pero pocos realmente la aplican y ahora se verifican sus consecuencias [dilema de Collingridge (Liebert *et al.*, 2010)]. La innovación sin restricciones y una legislación laxa de derechos de las personas de la Internet actual creó ecosistemas de grandes corporaciones, con enormes cantidades de datos personales en formatos diversos e incompatibles entre sí, que ahora deben ser "pseudonimizados" (el contexto es diferente en UE que en China). La persona ahora tiene el derecho de pedir la traza de sus datos y su uso, la explicación de los algoritmos por los cuales fueron procesados y el motivo. Estas cuestiones de ética no fueron contempladas en los requerimientos de los grandes ecosistemas de *Big Data*

o de servicios de IA especiales (perfiles y patrones) o de *Blockchain,* cada uno con sus enormes "almacenes" de datos, para que sean adaptables a las restricciones de cualquier mercado. Será muy costoso en tiempo, esfuerzo y dinero transformarlos. Las protestas y debates de que estas regulaciones frenan o destruyen las innovaciones y avances, en especial de IA, no van a tener efecto en una IoT global.

Las ventajas para las personas son que 1) desaparece el concepto de "caja negra", o sea, la falta de transparencia de los algoritmos de IA, en especial cuando estaban estrechamente vinculados a secretos comerciales o a prácticas cuasi ilegales o ilegales, como el caso de Cambridge Analytica (infobae, 2018). 2) Deberán identificarse y corregirse los sesgos (*biases*), que siempre fueron características no deseadas en un sistema de información (Friedman *et al.,*1997). Este es un problema generalizado que la industria no tomaba en cuenta y que en IoT podría haber tenido un impacto dañino sin precedentes, como comenta John Giannandrea (Knight, 2017), quien dirige IA en Google. Su preocupación era por los riesgos que podían generar los algoritmos de aprendizaje automático que aprenden los prejuicios humanos (sesgos) y que son utilizados para tomar millones de decisiones cada minuto. La verdadera cuestión de seguridad es que estos sistemas están trabajando con datos sesgados. Las consecuencias se pueden notar, por ejemplo, en el sistema COMPAS de Northpointe, que usa modelos de aprendizaje automático y predice la probabilidad de reincidencia de los acusados. Es utilizado por algunos jueces para determinar si se concede libertad condicional a un recluso. Una investigación de *ProPublica* encontró evidencia de que el modelo está sesgado en contra de las minorías (Spielkamp, 2017).

Sin embargo, emerge un nuevo riesgo. Taylor *et al.* (2017) advierten que *Big Data*, y la analítica de datos evolucionaron hacia otro nivel, la del análisis de grupos de personas, en el cual el individuo es incidental. Los riesgos ahora son a nivel colectivo, aún no está claro cuáles son los grupos o sociedades en riesgo. Algunas de las tipologías que exploraron son grupos colectivos políticos, grupos creados por algoritmos y grupos étnicos. Sin embargo, definir claramente qué es privacidad de un grupo o una sociedad en este ambiente, requiere de la filosofía legal, ética de la información, derechos humanos, computación, sociología y geografía, porque ahora se trata de tipos de datos digitalizados relacionadas con información genómica, redes sociales digitales, trazas de telefonía móvil, etc., sujetos a las nuevas posibilidades de análisis.

El uso puede ser para bien o para mal, porque facilitan monitorear y vigilar, que pueden estar dirigidos a proteger (derechos humanos, epidemio-

logía, etc.) o a controlar (seguridad, antiterrorismo). Permiten clasificar y categorizar por medio de perfiles, desde niveles de posibles amenazas a la seguridad, actividad disidente hasta información biométrica y asistencia sanitaria, mapeo de pobreza en países con bajos ingresos, etc., que trascienden las fronteras. Los conceptos de beneficio o perjuicio antes aplicados al individuo, ahora deberán aplicarse a los grupos. Si las políticas y las decisiones se hacen con base en estos nuevos perfiles y patrones, algunos grupos serán afectados positiva o negativamente. Los conceptos de Verbeek (2006) de "mediadores activos" y los "artefactos que tienen política" de Winner (1986) están más vigentes que nunca.

6. REFERENCIAS BIBLIOGRÁFICAS

Almeida, V. A., D. Doneda, y M. Monteiro (2015): "Governance challenges for the Internet of Things", en *IEEE Internet Computing*, 19 (4), pp. 56-59.

CERP-IoT (2009): "Internet of Things, strategic research roadmap", *Cluster of European Research Project European Commission*.

CPS PWG (2017): *NIST Framework for cyber-physical systems: Vol. 1, Overview,* National Institute of Standards and Technology, Special Publication.

DIGIT Act. (2017): *S.88 - DIGIT Act 115th Congress (2017-2018),* <https://www.congress.gov/bill/115th-congress/senate-bill/88>, consultado el 10 de marzo de 2018.

Dimov, D. (2013): "Differences between the privacy laws in the EU and the US", en *Management, Compliance y Auditing*, INFOSEC Institute, <https://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/#gref>, consultado el 10 de mayo de 2018.

Dusek, V. (2006): *Philosophy of technology: an introduction*, Malden, Blackwell.

EU Digital Agenda (2014): *The EU explained: digital agenda for Europe*, European Commission, Directorate-General for Communication Citizens information, Luxemburgo, Publications Office of the European Union.

EU ETICA Project (2011): "Towards Responsible Research and Innovation in the information and communication technologies and security technologies fields", en *A Report from the European Commission Services,* <http://www.etica-project.eu/>, consultado el 10 de abril de 2018.

EU GDPR (2018): "General data protection regulation - Reforma de 2018 de las normas de protección de datos de la UE", en *Justicia y*

derechos fundamentales, Comisión Europea, <https://ec.europa.eu/>, consultado el 10 de junio de 2018.

EU RRI (2012): *Responsible Research and Innovation: europe's ability to respond to societal challenges*, European Commission, Luxemburgo, Publications Office of the European Union.

European Commission (2010): *Europe 2020: a strategy for smart, sustainable and inclusive growth*, Bruselas, Comisión Europea, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF>, consultado el 10 de marzo de 2018.

Fabiano, N. (2017): "Internet of Things and blockchain: legal issues and privacy. The challenge for a privacy standard", en *Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE*, pp. 727-734.

Feenberg, A. (2003): "What is philosophy of technology?", Lecture at the University of Tokyo, Komaba campus.

Felt, U., B. Wynne, M. Callon, M. E. Gonçalves, S. Jasanoff, M. Jepsen, P. B. Joly, Z. Konopasek, S. May, C. Neubauer, A. Rip, K. Siune, A. Stirling y M. Tallacchini (2007): "Taking european knowledge society seriously", en *Report of the expert group on science and governance to the Science, Economy and Society Directorate,* Directorate-General for Research, European Commission, Bruselas, Directorate-General for Research, Science, Economy and Society.

Floridi, L. (2011): *The philosophy of information*, Oxford, Oxford University Press.

Floridi, L. (2015): *The onlife manifesto,* Oxford, Springer-Verlag GmbH.

Friedman, B. (Ed.). (1997): *Human values and the design of computer technology,* Cambridge, Cambridge University Press.

FTC Report (2015): *Internet of Things: Privacy and Security in a Connected World*, FTC Staff Report, enero de 2015.

Gartner (2017): "Gartner identifies the top 10 internet of things technologies for 2017 and 2018", en *Gartner Newsroom*, <https://www.gartner.com/newsroom/id/3221818>, consultado el 10 de marzo de 2018.

Gasiorowski-Denis, E. (2016): "How the Internet of Things will change our lives", en *ISO News*, 5 de septiembre de 2016.

Gavison, R. (1980): "Privacy and the limits of law", en *Yale Law Journal,* 9 (3), pp. 421-71.

Hawley, R. (1995): "Information as an asset: the board agenda", en *Information,* 28 (6), pp. 237-239.

HiPEAC (2015): "Internet of Things: technology and applications for a good society, thematic sesion", *European Network on High Performance and Embedded Architecture and Compilation*, NUST, Oslo.

Infobae (2018): "7 claves para entender el escándalo de Facebook y Cambridge Analytica", en *Tecno*, Infobae, <https://www.infobae.com/america/tecno/2018/03/20/7-datos-para-entender-el-escandalo-de-facebook-y-cambridge-analytica/>, consultado el 10 de marzo de 2018.

Infosec Institute (2017): *Overview of the proposed DIGIT act*., INFOSEC Institute.

IoTWF (2017): "Internet of Things world forum", <https://www.iotwf.com/iotwf2017/about>, consultado el 10 de enero de 2018.

Intel (2016): "Making the connection, how the Internet of Things engages consumers and benefits business", en *The Consumer Goods Forum, Capgemini and Intel*, <https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/how-iot-engages-consumers-benefits-business-paper.pdf>, consultado el 10 de mayo de 2018.

ITU-T Y.2060 (2012): "Overview of the Internet of Things", en *Series Y: Global information infrastructure, internet protocol aspects and next-generation networks. Next generation networks, frameworks and functional architecture models*, Telecommunication standardization sector of ITU.

ITU IoT (2005): "The Internet of Things, executive summary", en *ITU Internet Reports*.

Jasanoff, S. (2000): "Technological risk and cultures of rationality", en *Incorporating science, economics, and sociology in developing sanitary and phytosanitary standards in international trade,* National Research Council, National Academies Press.

Knight, W. (2017): "Forget killer robots Bias is the real AI danger", en *MIT Technology Review*, <https://www.technologyreview.com/s/608986/forget-killer-robotsbias-is-the-real-ai-danger/>, consultado el 10 de enero de 2018.

Krohn, W. y J. Weyer (1994): "Society as a laboratory, the social risks of experimental research", en *Science and Public Policy*, 21 (3), pp. 173-183.

Latour, B. (2005): *Reassembling the social: an introduction to actor-network-theory*, Oxford, Oxford University Press.

Liebert, W. y J. C. Schmidt (2010): "Collingridge's dilemma and techno-science", en *Poiesis & Praxis*, 7 (1-2), pp. 55-71.

Liao, T. (2018): "China publishes national standard for personal data protection", en *Morgan Lewis* & *Bockius*, <https://www.morganlewis.com/pubs/china-publishes-national-standard-for-personal-data-protection>, consultado el 10 de mayo de 2018.

Nicolescu, R., M. Huth, P. Radanliev y D. De Roure (2018): "Mapping the values of IoT", en *Journal of Information Technology*, pp. 1-16.

NIST (2017): "IoT security and privacy risk considerations", en *NIST Cybersecurity for IoT Program and Privacy Engineering Program,* <https://www.nist.gov/>, consultado el 10 de mayo de 2018.

Nye, D. E. (2006): *Technology matters: questions to live with,* Cambridge, MIT Press.

O'Brien, C. (2018): "Tech, regulation, and the strange new innovation scorecard at CES 2018", en *VentureBeats Newsletter*, <https://venturebeat.com/2018/01/11/tech-regulation-and-the-strange-new-innovation-scorecard-at-ces-2018/>, consultado el 10 de mayo de 2018.

O'Connor, N. (2018): "Reforming the U.S. approach to data protection and privacy", en *Digital and Cyberspace Policy Program*.

OTA (2017a): "Internet of Things: a vision for the future", en *Online Trust Alliance and the Internet Society* (ISOC), <https://otalliance.org/>, consultado el 10 de mayo de 2018.

OTA (2017b): "IoT security and privacy trust framework v2.5", en *Online Trust Alliance and the Internet Society* (ISOC), <https://otalliance.org/>, consultado el 10 de mayo de 2018.

Pinch T. J. y W. E. Bijker (2013): "La Construcción Social de la Tecnología", en *La construcción social de hechos y de artefactos: o acerca de cómo la sociología de la ciencia y la sociología de la tecnología pueden beneficiarse mutuamente*, Bernal, Universidad Nacional de Quilmes.

Regan, P. M. (1995): *Legislating privacy*, Chapel Hill, University of North Carolina Press.

Reydon, T. A. C. (2017): "Philosophy of Technology", en *IEP (Internet Encyclopedia of Philosophy),* <http://www.iep.utm.edu/technolo/>, consultado el 10 de enero de 2018.

Roessler, B y D. Mokrosinska (2013): "Privacy and social interaction", en *Philosophy & Social Criticism,* 39 (8), pp. 771-791.

Simitis, S. (1987): "Reviewing privacy in an information society", en *University of Pennsylvania Law Review,* 135 (3), pp. 707-746.

Spielkamp, M. (2017): "Inspecting algorithms for bias", en *Business Impact*, *MIT Technology Review*, <https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/>, consultado el 10 de mayo de 2018.

Sullivan, B. (2006): "'La difference' is stark in EU", NBCNEWS, <http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.WyqhIqkna3I>, consultado el 10 de mayo de 2018.

Taylor, L., L. Floridi, L. y B. van der Sloot (2017): "Introduction: a new perspective on privacy", *Group Privacy*, Springer, pp. 1-12.

Thielman, S. (2017): "Acting federal trade commission head; Internet of Things should self-regulate", en *Internet of Things, The Guardian*.

Thierer, A. (2013): "Privacy and security implications of the Internet of Things", en *Public Interest Comment,* Mercatus Center, George Mason University.

Thierer, A. (2017): "Does 'permissionless innovation' even mean anything?", en *The Technology Liberation Front.*

Van Baalen, P. J., P. C. van Fenema y C. Loebbecke (2016): "Extending the social construction of technology (SCOT) framework to the digital world", en *ICIS*.

Van de Poel, I. (2016): "An ethical framework for evaluating experimental technology", en *Science and engineering ethics*, 22 (3), pp. 667-686.

Verbeek, P. P. (2006): "Materializing morality: design ethics and technological mediation", en *Science, Technology, & Human Values*, 31 (3), pp. 361-380.

Winner, L. (1986): "Do artifacts have politics?", en *The Whale and the Reactor: A search for limits in an age of high technology,* Chicago, University of Chicago Press, pp. 19-39.

Whiteside, K. H. (2006): *Precautionary politics: principle and practice in confronting environmental risk*, Cambridge, MIT Press.

Wright, D., R. Gellert, S. Gutwirth y M. Friedewald (2011): "Precaution and privacy impact assessment as modes towards risk governance", en *Towards responsible research and innovation in the information and communication technologies and security technologies fields,* European Commission, Luxemburgo, Publications Office of the European Union.

Yoo, Y., O. Henfridsson y K. Lyytinen (2010): "Research commentary - the new organizing logic of digital innovation: an agenda for information systems research", en *Information systems research*, 21 (4), pp. 724-735.